Mr. Thomas, from the Committee on Ways and Means, submitted the following

REPORT

[To accompany H.R. 2971]

[Including cost estimate of the Congressional Budget Office]

The Committee on Ways and Means, to which was referred the bill (H.R. 2971) to amend the Social Security Act to enhance Social Security account number privacy protections, to prevent misuse of the Social Security account number, and to otherwise enhance protections against identity theft and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

		Page
I.	**Introduction**	3
	A. Purpose and Summary	3
	B. Background	3
	C. Legislative History	4
II.	**Section-by-Section Summary**	6
III.	**Vote of the Committee**	34
	A. Motion to Report the Bill	34
IV.	**Budget Effects of the Bill**	35
	A. Committee Estimates of Budgetary Effects	35
	B. Budget Authority and Tax Expenditures	35
	C. Cost Estimate Prepared by the Congressional Budget Office	35
V.	**Other Matters to be Discussed under the Rules of the House**	35
	A. Committee Oversight Findings and Recommendations	35
	B. Statement of General Performance Goals and Objectives	35
	C. Constitutional Authority Statement	36
	D. Information Relating to Unfunded Mandates	36
VI.	**Changes in Existing Law Made by the Bill, as Reported**	36

I. INTRODUCTION

A. PURPOSE AND SUMMARY

The purpose of the "Social Security Number Privacy and Identity Theft Prevention Act of 2004," H.R. 2971, is to enhance Social Security number privacy protections, prevent misuse of Social Security numbers (SSNs), and to otherwise enhance protections against identity theft.

The bill would restrict the sale, purchase and display to the general public of SSNs in the public and private sectors; provide additional measures to protect SSN privacy; ensure SSNs are assigned accurately; and create criminal and civil monetary penalties for persons who misuse SSNs.

B. BACKGROUND

The SSN was created in 1936 to track workers' earnings for the purpose of paying Social Security taxes and determining eligibility and benefit amounts upon retirement, or later upon disability. Since 1936, the Social Security Administration (SSA) has issued more than 400 million SSNs.

Although the SSN was originally created for administering the Social Security program, its use has expanded dramatically throughout both the public and private sectors. Federal use of the SSN was first mandated by President Roosevelt in 1943 with Executive Order 9397. This Executive Order required that any Federal department establishing a new system of permanent account numbers pertaining to an individual must exclusively utilize the SSN and that such personal information must be kept confidential. Today the SSN is required for the administration of a number of government benefit programs and the Federal income tax.

In addition to uses mandated by Federal law, the SSN is also widely used in the public and private sectors for purposes that are neither required nor prohibited by law. As a result, the SSN is generally regarded as the single-most widely used record identifier by both government and private sectors within the United States.

Ubiquitous use of SSNs and the ease with which individuals can access another person's SSN have raised serious concerns over privacy and opportunities for identity theft and fraud. The Federal Trade Commission (FTC), the SSA, the SSA Inspector General and others acknowledge that SSNs play a pivotal role in identity theft. Even worse, terrorists may steal, fake, or purchase SSNs in order to operate in our society and abet their nefarious acts. According to an FTC-sponsored survey conducted in March and April 2003, nearly 10 million people – or 4.6 percent of the adult population – discovered that they were victims of some form of identity theft in the past year, and it

collectively cost individuals and businesses more than $50 billion during that time period. Protecting the privacy of SSNs will help to protect our individual and national security.

The absence of overarching Federal law regulating the sale, purchase, and display to the general public of SSNs, and the growing threat represented by SSN misuse and identity theft, have prompted a need to better protect the privacy and integrity of SSNs.

C. LEGISLATIVE HISTORY

During the 106th Congress, the Subcommittee held hearings on Social Security program integrity on March 30, 2000 (106-38); representative payees on May 4, 2000 (106-57); use and misuse of Social Security numbers on May 9 and May 11, 2000 (106-108); and the processing of attorney's fees on June 14, 2000 (106-70). The information gained from these hearings led to the introduction of H.R. 4857, the "Privacy and Identity Protection Act of 2000" on July 13, 2000. The bill enhanced privacy protections for individuals, prevented fraudulent misuse of the Social Security number, and provided additional safeguards for Social Security and Supplemental Security Income beneficiaries with representative payees. A further hearing on protecting privacy and preventing misuse of the Social Security number was held on July 17, 2000 (106-43). On July 20, 2000, the Subcommittee on Social Security ordered favorably reported H.R. 4857, as amended. The Committee on Ways and Means ordered the bill favorably reported, as amended on September 28, 2000 (H. Rept. 106-996 Part 1). The bill was not considered by the full House, as other committees of jurisdiction did not complete consideration of the bill.

During the 107th Congress, the Subcommittee held a hearing on protecting privacy and preventing misuse of Social Security numbers on May 22, 2001 (107-31). In response to information gathered at this hearing and previous hearings in the 106th Congress, Subcommittee Chairman E. Clay Shaw, Jr., introduced H.R. 2036, the "Social Security Number Privacy and Identity Theft Prevention Act of 2001" on May 25, 2001. The bill restricted the sale, purchase, and display of Social Security numbers, limited dissemination of Social Security numbers by credit reporting agencies, and made it more difficult for businesses to deny services if a customer refused to provide his or her Social Security number. Further hearings were held on preventing identity theft by terrorists and criminals, held jointly with the Committee on Financial Services, Subcommittee on Oversight and Investigations on November 8, 2001 (107-51); protecting the privacy of Social Security numbers and preventing identity theft on April 29, 2002 (107-71); and preserving the integrity of Social Security numbers and preventing their misuse by terrorists and identity thieves, held jointly with the Committee on Judiciary, Subcommittee on Immigration, Border Security, and Claims on September 19, 2002 (107-81). Neither the House nor the Senate acted on the bill.

During the 108th Congress, the Subcommittee held a hearing on the use and misuse of Social Security numbers on July 10, 2003 (108-35). The General Accounting Office (GAO) witness testified that SSNs are widely utilized in both the public and private sectors as an identifier, and cited numerous examples where public and private databases had been compromised and personal data, including SSNs, had been stolen. They also found that in some cases, the display of SSNs in public records and easily accessible websites provided an opportunity for identity thieves. The SSA Inspector General testified that the most important step in preventing SSN misuse is to limit its easy availability through public records, sale on the open market, and unnecessary use. Consumer advocate witnesses testified regarding the growing crime of identity theft, its impact on victims, and the need to protect the privacy of SSNs. A law enforcement witness testified that SSNs are key to the takeover of another individual's identity, described difficulties in prosecuting identity theft, and stated the need to restrict SSN use to necessary purposes.

Based on information gathered at this hearing and hearings in previous Congresses, Subcommittee Chairman E. Clay Shaw, Jr. introduced H.R. 2971, the "Social Security Number Privacy and Identity Theft Prevention Act of 2003" on July 25, 2003. The bill was referred to the Committee on Ways and Means, the Committee on Financial Services, and the Committee on Energy and Commerce. The Subcommittee held a further hearing on enhancing Social Security number privacy on June 15, 2004, and marked up the bill on July 15, 2004. The bill was reported favorably to the full Committee on Ways and Means on July 15, 2004, as amended, by voice vote. On July 21, 2004, the Committee on Ways and Means marked up H.R. 2971, as amended by the Subcommittee. Chairman Thomas offered an amendment in the nature of a substitute, which was agreed to by voice vote. The Committee then ordered favorably reported H.R. 2971, as amended, by a roll call vote of 33 ayes to 0 nays.

In addition, during the 106th, 107th, and 108th Congresses, Subcommittee Chairman Shaw asked the GAO for a number of reports to inform the debate on SSN privacy and integrity. He requested several reports explaining how government agencies and private sector businesses such as consumer reporting agencies, information resellers, and health care organizations collect, utilize, and safeguard SSNs (*Social Security, Government and Commercial Use of the Social Security Number is Widespread*, GAO/HEHS-99-28; *Social Security Numbers, Government Benefits from SSN Use But Could Provide Better Safeguards*, GAO-02-352; *Social Security Numbers, Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information*, GAO 04-11; *Social Security Numbers, Use is Widespread and Protections Vary*, GAO-04-768T). He also requested a report on the Social Security Administration's vulnerabilities to error and fraud in issuing SSNs to noncitizens and initiatives to address these vulnerabilities (*Social Security Administration, Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens But Some Weaknesses Remain*, GAO-04-12).

II. SECTION-BY-SECTION SUMMARY

Sec. 1. Short title

Current Law:

No provision.

Explanation of Provision:

Section 1 provides that the Act may be cited as the "Social Security Number Privacy and Identity Theft Prevention Act of 2004."

Reason for Change:

The section identifies the short title for the bill.

TITLE I--PROVISIONS RELATING TO THE SOCIAL SECURITY ACCOUNT NUMBER IN THE PUBLIC AND PRIVATE SECTORS

Sec. 101. Restrictions on the sale or display to the general public of Social Security account numbers by governmental agencies.

Current Law:

The SSN is required by law for the administration of a number of Federal programs. In addition, Federal law permits States to require the SSN in the administration of certain State programs, and in other cases Federal law requires the States to use the SSN in the administration of Federal or State programs. No Federal law regulates the overall use of SSNs by Federal, State or local governments. The "Department of Transportation and Related Agencies Appropriations Act" (P.L. 106-346) amended the "Driver's Privacy Protection Act of 1994" (P.L. 103-322) to require States to obtain express consent of drivers before sharing or selling drivers' "highly restricted personal information," including SSNs, except under very limited circumstances.

Explanation of Provision:

The bill would restrict the sale or display to the general public of full or partial SSNs by Federal, State or local governmental agencies and their agents, or by a bankruptcy trustee. The sale of SSNs would be permitted as follows:

1. As specifically authorized by the "Social Security Act" (P.L. 74-271);
2. For law enforcement or national security purposes;

3. For tax compliance;
4. By State departments of motor vehicles for use by a government agency in carrying out its functions; for use by an insurer for claims investigation, anti-fraud activities, and rating or underwriting; and for use by an employer to obtain or verify information about a holder of a commercial driver's license;
5. To a consumer reporting agency under the "Fair Credit Reporting Act" (FCRA) (P.L. 91-508) solely for use or disclosure for permissible purposes under the FCRA as follows: as ordered by a court or a Federal grand jury subpoena; as instructed by the consumer in writing; for the extension of credit based on a consumer's application; for review or collection of a consumer's account; for employment purposes (with the consumer's permission); for insurance underwriting based on a consumer's application; when there is a legitimate business need to process a transaction the consumer initiates; to review whether a customer meets the terms of his or her account; to determine a consumer's eligibility for a license or other benefit granted by a government agency; to analyze the credit or prepayment risks associated with an existing credit obligation; and for use by State and local officials for child support payment purposes;
6. For government research advancing the public good.

In addition, the U.S. Attorney General would be permitted to authorize sale and display to the general public of SSNs in other circumstances as determined appropriate.

The restrictions on sale or display to the general public of SSNs would not apply to SSNs of deceased persons.

The restrictions that would be established under this provision would not override other restrictions or limitations in Federal law or regulations to the extent that current law provides greater protections for SSNs than would be created under this provision in the bill.

The bill would define "sell" as accepting an item of material value in exchange for an SSN. "Display to the general public" would mean to intentionally place an SSN in a viewable manner on an Internet site that is available to the general public or to provide access to the general public by other means. In addition, requiring an individual to transmit his or her SSN over the Internet without ensuring the number is encrypted or otherwise protected would be considered a prohibited display to the general public. "Social Security account number" would include a partial SSN, except for the last 4 digits for a period of 6 years after the deadline to issue regulations implementing the provisions.

Reason for Change:

The government created the SSN and requires its use for a broad range of interactions between individuals and the government, including tax administration, many benefit programs, and driver's and professional licenses. While there are laws protecting the privacy of SSNs held by certain agencies or under specific circumstances, there is no comprehensive law protecting the privacy of SSNs held by Federal, State, and local government agencies. As a result, SSNs may be sold, displayed on the Internet, or otherwise made available to the general public on paper, computer disk, or other means to individuals requesting a copy—for example through open court or other government records—and may be obtained by third parties who can subsequently sell or display the information to others.

Since SSNs are the key to accessing an individual's financial and other personal information, the wide accessibility of SSNs has raised serious concerns over privacy. Testimony before the Subcommittee on Social Security highlights the relative ease by which an individual can obtain another person's SSN and use the information to commit identity theft or other crimes. Restricting the display to the general public and sale of SSNs by governments will help curb fraudulent activity by making it more difficult for criminals to access this personal information.

The bill would provide specific exceptions to permit the continuation of SSN exchanges that provide important benefits in the public interest—such as law enforcement (including child support enforcement); administration of government programs, including Supplemental Security Income, Medicaid, and unemployment insurance; limited commercial purposes such as granting credit and insurance; tax administration; and government research advancing the public good. In addition, authority would be given to the U.S. Attorney General to authorize sale and display to the general public of SSNs as determined appropriate under guidelines specified in Section 102 of the bill. Since SSN use is so pervasive in both the public and private sector, is linked to so many government and business transactions, and because of evolving needs regarding SSN utilization and new technologies to facilitate information exchanges, this exception is intended to allow the U.S. Attorney General or agencies to which it delegates authority to thoroughly evaluate how SSNs are sold and displayed, the degree to which they are convenient versus essential to such exchanges, and to modify the rules as needed. However, it is expected that this authority would be used extremely judiciously, and not merely for the sake of facilitating transactions or data-matching that could be reasonably accomplished without the use of the SSN. In comparing the costs and benefits of authorizing SSN sale or display to the general public, it is expected that the U.S. Attorney General and other agencies would give significant weight to the need to maintain individuals' privacy and safety, as well as the bill's purpose of preventing identity theft.

With respect to the exception for research advancing the public good, the intent is to preserve the government's ability to conduct scientific, epidemiological, and social scientific research that would benefit the public. In the case of research involving medical information on individuals, it is expected that the SSA and the U.S. Attorney General will only authorize sale of SSNs in strict compliance with Federal rules and regulations on the privacy of medical information.

The restrictions on sale and display to the general public of SSNs would not apply to the SSNs of deceased persons. This is because the sale and public availability of information on deceased individuals is necessary to prevent waste, fraud, and abuse. The SSA compiles a Death Master File (DMF), which contains the name, date of birth, date of death, SSN, and other information for about 70 million individuals. The SSA DMF is used by leading government, financial, investigative, and credit reporting organizations, in medical research and by other industries to verify identity as well as to prevent fraud and comply with the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act) (P.L. 107-56).

The restrictions on sale and display by government agencies, trustees, and their agents would only apply to SSNs they require individuals or others to provide. During Social Security Subcommittee hearings on the bill, court and other public records administrators testified they receive numerous documents filed by individuals, businesses, and attorneys that often include SSNs the government did not require to be submitted, and of which they are therefore unaware. They stated redaction of "incidentally" included SSNs would create a serious administrative burden, and it would require significant resources to review each document and redact such incidental SSNs. Therefore, the bill would make government agencies, trustees, and their agents responsible only for those SSNs they require individuals to submit, since they should be able to easily locate and redact them. For example, a court requiring individuals to provide their SSNs on a coversheet for filed documents could remove the coversheet or redact the SSN before selling the court record or displaying it to the general public. With respect to SSNs submitted in court documents absent the court's requirement to do so, the individual communicating the SSN in the document, not the court, would be held responsible according to Section 108 of the bill.

The restrictions established under this bill would serve as a floor of protection for SSNs, and are not intended to override SSN protections in current Federal law or regulations to the extent they provide greater restrictions on SSN sale, purchase, or display to the general public than would be created under the bill. For example, this bill is not intended to circumvent the provision included in the "Food, Agriculture, Conservation, and Trade Act of 1990," (P.L. 101-624) preventing the disclosure of SSNs maintained as the result of laws enacted on or after October 1, 1990.

Effective Date:

Final regulations to carry out the new restrictions on SSN sale and display to the general public created in this section of the bill would have to be issued by the Commissioner of Social Security (hereafter referred to as the Commissioner), the U.S. Attorney General, or any other agency to which the U.S. Attorney General delegates authority within 18 calendar months after the date of enactment. The provisions would take effect one year after issuance of regulations. The provisions would not apply to records generated prior to the date the provisions become effective.

Sec. 102. Regulatory authority.

Current Law:

No provision in current law.

Explanation of Provision:

The bill would direct the U.S. Attorney General to issue regulations regarding the sale, purchase, or display to the general public of SSNs and to provide an opportunity for public comment on regulations in accordance with the "Administrative Procedure Act" (P.L. 79-404). The U.S. Attorney General would be required to consult with the Commissioner, the Secretary of Health and Human Services the Secretary of Homeland Security, the Secretary of the Treasury, the Federal Trade Commission, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Securities and Exchange Commission, State attorneys general and representatives of the State insurance commissioners as designated by the National Association of Insurance Commissioners.

When authorizing the sale, purchase, or display of SSNs for law enforcement or national security purposes, the U.S. Attorney General would be required to find that the sale, purchase or display would serve a compelling public interest that cannot reasonably be served through alternative measures, and would not pose an unreasonable risk of identity theft, or harm to an individual.

The U.S. Attorney General would be able to authorize the sale, purchase, or display to the general public of SSNs for purposes other than law enforcement or national security, only after considering the costs and benefits to the general public, businesses, commercial enterprises, non-profit associations, and governments. If the U.S. Attorney General authorizes the sale, purchase, or display to the general public of SSNs, he or she would be required to impose restrictions and conditions to reduce the likelihood of fraud

and crime and to prevent an unreasonable risk of identity theft or bodily, emotional or financial harm to individuals.

Reason for Change:

The SSN is widely used throughout the public and private sectors. Some uses are authorized or required under law, others are to facilitate data-matching and record-keeping, and still others are simply for convenience's sake. The development of coordinated regulations regarding SSN sale, purchase, and display across such diverse agencies and businesses makes it necessary to centralize regulatory authority with the SSA (which is responsible for issuing SSNs) and the U.S. Attorney General (which enforces criminal penalties with respect to SSN misuse under current law). In addition, the U.S. Attorney General would have authority to delegate rulemaking to other Federal agencies as appropriate, and would facilitate coordinated and consistent rulemaking.

In addition, to address concerns that the limited list of exceptions does not enumerate all instances in which the sale, purchase, and display of SSNs may be essential and irreplaceable for government and business transactions, the U.S. Attorney General would be given authority to authorize the sale, purchase or display to the general public of SSNs. The legislation provides guidelines to ensure SSNs are exchanged only when there is no other alternative that could reasonably accomplish the objective, and with due consideration for the unintended and potentially harmful consequences to individuals, government agencies, and businesses that may result.

Effective Date:

The regulatory authority would be effective upon enactment.

Sec. 103. Prohibition of display of Social Security account numbers on checks issued for payment by governmental agencies.

Current Law:

No Federal law regulates the overall use of SSNs by Federal, State, or local governments. However, the "Social Security Number Confidentiality Act of 2000" (P.L. 106-433) specifically directed the Secretary of the Treasury to take necessary action to ensure that SSNs are not visible on or through unopened mailings of checks or other drafts.

Explanation of Provision:

The bill would prohibit Federal, State, or local governments, or bankruptcy trustees, from including full or partial SSNs on checks issued for payment or on any documents accompanying checks.

Reason for Change:

The Subcommittee has heard testimony from the Postal Inspection Service and consumer advocates that mail theft and rifling through trash for discarded documents are means by which identity thieves gain access to personal information, including SSNs.

Effective Date:

Would apply with respect to checks (and documents attached to or accompanying such checks) issued after one year after enactment.

Sec. 104. Prohibition of the display of Social Security account numbers on driver's licenses or motor vehicle registrations

Current Law:

Many States have acted voluntarily to prohibit the display of SSNs on driver's licenses or other identification cards; however some States have made changing from an SSN to another number an option, but not a requirement.

Explanation of Provision:

The bill would prohibit States and their political subdivisions from placing a person's full or partial SSN on a driver's license, motor vehicle registration, or on any other document issued for purposes of identification of an individual. This would include use of a magnetic strip, bar code, or other means of communication to convey the full or partial SSN.

Reason for Change:

The Subcommittee has heard testimony that loss or theft of driver's licenses or motor vehicle registrations that display the SSN contributes to identity theft. In addition, identity thieves may obtain bar code readers or other equipment that enables them to access SSNs that are stored in magnetic strips, bar codes, or smart chips on driver's licenses. However, this provision is not intended to prevent inclusion of encrypted SSNs (those that are transformed by a secret code to appear as other than the nine-digit number

assigned by the Commissioner of Social Security when read or otherwise accessed by unauthorized parties).

Effective Date:

Would apply to licenses, registrations, and other documents issued or reissued after one year after enactment.

Sec. 105. Prohibition of the display of Personal Identification Numbers on government employee identification cards or tags.

Current Law:

No provision.

Explanation of Provision:

The bill would prohibit government agencies and those providing employee benefits for the government agency from displaying an individual's full or partial SSN on any identification card or tag issued to the employee or an employee's family member. This would include use of a magnetic strip, bar code, or other means of communication to convey the full or partial SSN.

Reason for Change:

SSNs are often utilized as employee identification numbers or customer account numbers for the sake of convenience. However, the display of SSNs on military identification tags, employee identification cards, health benefit cards, customer cards, and on other cards or tags that are required to be submitted or displayed to others unnecessarily increases the risk of identity theft. Similar prohibitions have been enacted under several State laws. However, this provision is not intended to prevent inclusion of encrypted SSNs (those that are transformed by a secret code to appear as other than the nine-digit number assigned by the Commissioner of Social Security when read or otherwise accessed by unauthorized parties).

Effective Date:

Would apply with respect to cards or tags issued after one year after enactment.

Sec. 106. Prohibition of inmate access to Social Security account numbers.

Current Law:

No provision.

Explanation of Provision:

The bill would prohibit Federal, State or local governments from employing prisoners in any capacity that would allow prisoners access to the SSNs of other individuals.

Reason for Change:

Prisoners, including those who may have been incarcerated for identity theft, should not have access to SSNs, thereby posing a serious risk of identity theft or fraud. The Subcommittee has heard testimony regarding a serious instance where use of prisoner labor to process personal information resulted in a case of stalking (*Beverly Dennis, et al. v. Metromail, et al., No. 96-04451, Travis County, Texas).*

Effective Date:

Would apply with respect to employment or entry into contract for employment of prisoners on or after enactment. In the case of employment or contracts for employment in effect on the date of enactment, the prohibition would take effect 90 days after enactment.

Sec. 107. Measures to preclude unauthorized disclosure of Social Security account numbers and protect the confidentiality of such numbers.

Current Law:

No provision.

Explanation of Provision:

With respect to Federal, State, and local government employees, the bill would restrict access to SSNs to employees whose responsibilities require access for administration or enforcement of the government agency's functions. Government agencies would be required to provide safeguards to prevent unauthorized access to SSNs and protect their confidentiality.

Reason for Change:

There have been numerous reported cases of computer hackers obtaining SSNs from universities and other institutions. In addition, the Subcommittee has heard testimony on how identity theft rings may plant an employee inside an organization to access SSNs and personal information.

Government agencies often ask or require individuals to provide their SSN to obtain benefits or services. Therefore, they have a responsibility to safeguard SSNs from unauthorized access by employees or other individuals.

This provision is not intended to prevent government employees or those to whom government agencies contract work from accessing SSNs in cases where it is necessary for performance of their duties, or to impede data exchanges between government agencies that include SSN information and are in accordance with Section 101 of the bill. For example, it is not the intent to prevent State unemployment insurance agencies from sending wage records or claim information to other Federal, State, or local government agencies (e.g. for purposes of determining eligibility or benefit amounts for Temporary Assistance to Needy Families, Housing and Urban Development assistance, Food Stamps, Supplemental Security Income, etc.).

Effective Date:

Would take effect one year after the date of enactment.

Sec. 108. Prohibition of the sale, purchase, and display to the general public of the Social Security account number in the private sector.

Current Law:

The Gramm-Leach-Bliley Act (GLBA)(P.L. 106-102) restricts the ability of financial institutions to disclose nonpublic personal information about consumers, including SSNs, to nonaffiliated third parties. The "Health Insurance Portability and Accountability Act" (HIPAA) (P.L. 104-191) Privacy Rule limits health plans, health care clearinghouses, and health care providers in disclosing certain protected information, including SSNs. Individuals must give specific authorization before health care providers and other covered entities may disclose protected information in most non-routine circumstances. However, no Federal law regulates the overall sale, purchase, and display to the general public of SSNs in the private sector.

Explanation of Provision:

The bill would prohibit the sale, purchase or display to the general public of an SSN. It also prohibits using an SSN to find an individual with the intent to injure or harm the individual, or using the individual's identity for illegal purposes.

A person who violates this section would be guilty of a felony, subject to fines under Title 18 of the United States Code and/or imprisonment for up to five years.

The bill would provide exceptions to the prohibitions on SSN sale and purchase for law enforcement; national security; public health; emergency health safety; tax compliance; by or to a consumer reporting agency for use or disclosure for permissible purposes described in the Fair Credit Reporting Act; and research (for advancing the public good and with restrictions to protect privacy of individuals).

The bill would also provide exceptions for sale, purchase, and display to the general public of SSNs with the affirmative written consent of the individual, and under other circumstances determined appropriate according to regulations issued by the U.S. Attorney General.

These prohibitions would not apply to SSNs of deceased persons.

The bill would also prohibit disclosure of the SSN to government agencies absent a request to do so or the individual's written permission, except for law enforcement (including child support enforcement) or national security purposes.

In addition, the bill would prohibit the display of full or partial SSNs on employee identification cards or tags, or cards or tags businesses and others require individuals to use to access goods and services.

The bill would require businesses and others that collect and store SSNs to prevent unauthorized access by employees or other individuals.

The restrictions that would be established under this provision would not override other restrictions or limitations in Federal law to the extent that current law provides greater protections for SSNs than would be created under this provision in the bill.

The bill would define "sell" as obtaining directly or indirectly anything of value in exchange for the SSN. "Purchase" would mean to provide, directly or indirectly, anything of value in exchange for the SSN. The terms "sell" and "purchase" would not include submission of the SSN when applying for government benefits or programs, use of SSNs in administration of employee benefit plans, or the sale, lease, merger, transfer, or exchange of a trade or business.

"Display to the general public" would mean to intentionally place an SSN in a viewable manner on an Internet site that is available to the general public or to provide access to the general public by other means. In addition, requiring an individual to transmit his or her SSN over the Internet without ensuring the number is encrypted or otherwise protected would be considered a prohibited display to the general public.

"Social Security account number" would include a partial SSN, except for the last 4 digits for a period of 6 years after the deadline to issue regulations to implement the provisions.

Reason for Change:

Use of SSNs in the private sector has proliferated for purposes unrelated to administration of the Social Security program, collection of taxes, or other purposes authorized under Federal law. Businesses may request a person's SSN as a condition of providing goods or services. Information resellers and consumer reporting agencies obtain SSNs and other personal information from customers, public records, and other sources to determine an individual's identity and accumulate information about them in order to provide that information to businesses or others for a fee. As a result, Americans are increasingly concerned that the SSN they disclose for one purpose may be subsequently sold to third parties and used for other purposes without their knowledge or consent. For example, an individual discloses his SSN to get a bank loan. The bank sends the information to a consumer reporting agency to request a credit report. The consumer reporting agency assembles information on the individual and associates it with the SSN. The consumer reporting agency may then incidentally or purposefully sell the SSN and other information to insurance companies, credit companies, information resellers, law enforcement, government agencies, private investigators, and others.

In addition, such widespread use of SSNs increases the risk that business employees, computer hackers, or others may obtain unauthorized access and misuse SSNs to commit identity theft or other crimes. According to an FTC-sponsored survey in 2003, among identity theft victims who knew the identity of the criminal, 23 percent said the person responsible worked at a company or financial institution that had access to the victim's personal information.

The bill would restrict the sale, purchase, and display to the general public of SSNs (examples of display to the general public, in addition to display over the Internet, would include making copies of SSNs available on paper, computer disk, or other media). The bill would also require that SSNs be appropriately safeguarded when collected and stored. The intent is to limit transmission of SSNs in order to minimize opportunities for SSN misuse and identity theft.

In limiting the transmission of SSNs, it is not the intent to prevent individuals from voluntarily providing their own SSN to facilitate a transaction that they initiate or to prevent businesses from utilizing SSNs in a transaction that the individual authorizes. For example, if an individual voluntarily gives his or her own SSN to a business so that it may provide goods or services, is not the intent of the bill to call such an exchange the "sale" or "purchase" of the SSN simply because it is facilitating the transaction.

In addition, during the course of the Subcommittee's consideration of the bill, the Federal Deposit Insurance Corporation (FDIC) expressed concern that the bill's restrictions on sale and purchase of SSNs could be interpreted to impede the FDIC's resolution or liquidation of failed insured depository institutions. However, the bill's language clarifying that "sell" or "purchase" does not include the sale, lease, merger, transfer, or exchange of a trade or business is intended to make clear that the FDIC may share SSNs in carrying out its responsibilities.

The bill would provide specific exceptions to the restrictions on sale and purchase of SSNs for law enforcement; national security; emergency health situations; public health; compliance with tax laws; for certain credit, insurance, and employment purposes; and research for advancing the public good. The bill would provide exceptions to restrictions on sale, purchase, and display to the general public of SSNs with the individual's voluntary and affirmative consent and under circumstances deemed appropriate by the U.S. Attorney General.

With respect to the exception for research advancing the public good, the intent is to preserve the government's ability to conduct scientific, epidemiological, and social scientific research that would benefit the public. It is not intended to facilitate private commercial research for product or service development or marketing. In the case of not-for-profit or other research advancing the public good, the U.S. Attorney General would have the ability to authorize SSN sale and purchase where appropriate in accordance with Section 102 of the bill. In the case of research involving medical information on individuals, it is expected that the SSA and the U.S. Attorney General will only authorize sale of SSNs in strict compliance with Federal rules and regulations on the privacy of medical information.

With respect to the exception for affirmative written consent of the individual, the intent is to enable individuals to authorize the sale, purchase, and display to the general public of their own SSNs if they determine it is in their own best interest. For example, an individual may choose to provide his or her SSN to a business and authorize the SSN's sale in order to speed up a transaction. Businesses and others soliciting such consent from the individual must explain clearly and understandably what giving consent would entail and the uses that might be made of the individual's SSN. Preferably, the explanation and solicitation of consent would be a distinct document or other communication separate from other explanations or solicitations from the business or

other persons. The terms of consent, and the explanation of the right to refuse consent or to limit the SSN's exchange solely to a specific transaction, should not be obscured by other explanations, authorizations, solicitations or other text that might be included in the same document. No individual should be obligated to provide consent; however, businesses and others may provide an explanation of the advantages and disadvantages (with equal prominence given to both) of providing versus refusing consent.

With respect to the exception permitting the U.S. Attorney General to authorize SSN sale, purchase, and display to the general public, for the same reasons discussed under Section 101, the expectation is that this authority would be used extremely judiciously and only when there are no other reasonable alternative measures that could attain the same objective.

For the same reasons discussed under Section 105, the bill would prevent private sector employers and those providing employee benefits from displaying an individual's full or partial SSN on any identification card or tag issued to the employee or an employee's family member. In addition, the bill would prevent businesses from displaying full or partial SSNs on cards or tags used to access goods and services. Individuals who must carry such cards and tags with their SSNs are at greater risk of identity theft should their wallets or purses be stolen or lost. According to an FTC-sponsored survey, 14 percent of identity theft victims said their personal information was obtained from a lost or stolen wallet, or checkbook.

Section 101 of the bill would prohibit government agencies from selling or displaying to the general public SSNs they require individuals to disclose to the government. However, many of the SSNs that appear in government records, particularly court records, result from attorneys, title companies, or other businesses and individuals including a person's SSN on papers submitted to the court for convenience's sake. Government agencies do not have the resources to comb through innumerable documents searching for such "incidental" inclusion of SSNs. As a result, an individual's SSN could be displayed to the public without the individual realizing it. Therefore, to prevent inadvertent sale or display of SSNs by government agencies, the bill would prohibit the submission of the SSN to government agencies absent the government agency's requiring that the number be submitted or the individual's written consent.

The restrictions on private sector sale, purchase, and display to the general public of SSNs would not apply to the SSNs of deceased persons. This is because the sale and public availability of information on deceased individuals is necessary to prevent fraud. As mentioned in the discussion under Section 101, the SSA DMF is used by both public and private sector entities to prevent fraud and comply with the USA PATRIOT Act. By methodically running financial, credit, payment and other applications against the DMF, the financial community, insurance companies, security firms and State and local governments are better able to identify and prevent identity fraud. The USA PATRIOT

Act requires an effort to verify the identity of customers, including procedures to verify customer identity and maintaining records of information used to verify identity.

As discussed under Section 101, this bill is intended to serve as a floor of protection for SSNs and is not intended to override SSN protections in current Federal law or regulations to the extent they provide greater restrictions. For example, this bill is not intended to enable SSN sale, purchase, or display to the general public by health providers that would otherwise be prohibited under the HIPAA Privacy Rule.

Effective Date:

Final regulations to carry out the new restrictions on SSN sale, purchase, and display to the general public created in this section of the bill would have to be issued by the Commissioner, the U.S. Attorney General, or any other agency to which the U.S. Attorney General delegates authority within 18 calendar months after the date of enactment. The provisions would take effect one year after issuance of regulations.

Sec. 109. Confidential treatment of Credit Header information.

Current Law:

The Fair Credit Reporting Act (FCRA) imposes certain restrictions on the disclosure of "consumer report" information. However, information at the top of the credit report, known as "credit header" information, which includes SSNs, is not subject to these restrictions. The GLBA imposed some restrictions on release of credit header information, but the exceptions under which SSNs may be released under the GLBA are broader than the permissible purposes for which a consumer report may be released.

Explanation of Provision:

The bill would include the SSN in the definition of "credit report" under the FCRA so that the SSN receives the same privacy protections as other consumer credit information.

Reason for Change:

Consumer reporting agencies compile information on individuals' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. This highly personal information may be released only for purposes specified in the FCRA, such as credit issuance, insurance, employment, review of consumer accounts, certain government licenses or benefits, child support determinations, and other business transactions.

SSNs are the key to accessing information in a credit report, and deserve the same protection as the information itself. While the GLBA affords SSNs some protections, consumer reporting agencies may sell credit header information, including the SSN, for purposes beyond those permitted under the FCRA for credit reports or for a purpose beyond that for which the SSN was provided, thus increasing the risk SSNs will be used for identity theft or other crimes.

Effective Date:

Would take effect 90 days after enactment.

Sec. 110. Refusal to do business without receipt of Social Security account number considered unfair or deceptive act or practice.

Current Law:

No provision.

Explanation of Provision:

The bill would make it an unfair or deceptive act or practice in violation of the Federal Trade Commission Act (15 U.S.C. §45) for any person to refuse to do business with an individual because the individual will not provide his or her SSN. An exception is provided where the SSN is expressly required under Federal law.

Reason for Change:

Businesses may currently request a customer's SSN without being required to collect it under current law. They may also refuse to provide goods or services if the customer refuses to provide it. Once a business obtains a customer's SSN, there may be little or no oversight or regulation over how that business uses or shares that key piece of personal information, depending on the type of business.

The FTC, the SSA, and others warn individuals to avoid supplying an SSN and ask businesses to use another number whenever possible. Such warnings are justified, as the Subcommittee has heard testimony discussing identity theft abetted by unauthorized access to personal information by business employees.

Effective Date:

Would apply to acts or practices committed after 180 days after enactment.

TITLE II--MEASURES TO ENSURE THE INTEGRITY OF APPLICATIONS FOR SOCIAL SECURITY ACCOUNT NUMBERS AND REPLACEMENT SOCIAL SECURITY CARDS

Sec. 201. Independent verification of birth records provided in support of applications for Social Security account numbers.

Current Law:

Section 205(c)(2)(B)(ii) of the Social Security Act directs the Commissioner to require persons applying for an SSN to provide documentary evidence necessary to establish the individual's age, true identity, U.S. citizenship or lawful alien status, and any previously assigned SSNs. Section 205(c)(2)(A) of the Social Security Act specifies that information obtained by or submitted to the Commissioner shall be subject to verification as the Commissioner deems necessary.

As of 2002, SSA policy requires field office staff to obtain independent third-party verification of birth records for U.S.-born citizens age one and older. SSA policy does not require independent verification of birth records for children under age one (in such cases birth records are subject to visual inspection only).

In addition, SSA policy requires independent third-party verification of the immigration and work status of non-citizens before issuing an SSN.

Explanation of Provision:

The bill would direct the Commissioner to require independent verification of birth records provided by individuals applying for an SSN, except in cases of enumeration at birth. The bill would authorize the Commissioner to issue regulations to provide reasonable exceptions to this requirement in cases where the Commissioner determines there is minimal opportunity for fraud.

In addition, the bill would require the Commissioner to undertake a study to determine the feasibility and cost effectiveness of verifying all identification documents submitted by persons applying for a *replacement* Social Security card, including the feasibility and cost of developing electronic processes for third party verification of documents issued by Federal, State and local agencies.

Reason for Change:

In testimony before the Subcommittee, the General Accounting Office (GAO) stated that the SSA's policies related to assigning SSNs to children under age one could be exploited by individuals seeking fraudulent SSNs. GAO investigators working

undercover were able to obtain two SSNs by posing as parents of newborns and using counterfeit documents.

Audits and testimony by the SSA Inspector General also identified the assignment of SSNs to children as prone to fraud. In a 2000 audit, the SSA Inspector General reviewed over 3,500 original SSNs issued, and found 999 (28 percent) were assigned based on invalid or unacceptable documents. Of those, 56 SSN cards were issued to non-existent children.

Effective Date:

The provision requiring independent verification of birth records for newly issued SSNs would take effect with regard to applications for SSNs filed after 270 days after the date of enactment. The Commissioner would be required to report the results of the study on requiring verification of all identification documents for replacement SSN cards no later than two years after enactment.

Sec. 202. Enumeration at birth.

Current Law:

In States where the SSA has entered into an agreement, parents may request that the SSA assign an SSN to a newborn child as part of the official birth registration process (the parent need not fill out an SSN application form). In such cases, the State vital statistics office electronically transmits the request along with the child's name, date and place of birth, sex, mother's maiden name, father's name (if shown), address of the mother and birth certificate number to the SSA's central office in Baltimore. The SSA uses the birth registration information to establish the age, identity, and U.S. citizenship of the newborn child. The SSA then assigns an SSN to the child and sends the SSN card to the child at the mother's address.

Explanation of Provision:

The bill would require the Commissioner to make improvements to the application process for SSNs issued to newborns. Specifically, the improvements would be designed to prevent (a) assignment of SSNs to unnamed children; (b) issuance of more than one SSN to the same child; and (c) other opportunities for obtaining an SSN fraudulently.

In addition, the bill would require the Commissioner to undertake a study to determine options for improving the enumeration at birth process, including an examination of methods available to reconcile hospital birth records with birth

registrations submitted to State and local government agencies and information provided to the SSA.

Reason for Change:

Nearly 4 million SSNs (more than 70 percent of new SSNs) were issued through the enumeration at birth (EAB) program in fiscal year 2003. However, a 2001 audit by the SSA Inspector General found several weaknesses in the EAB program. The SSA Inspector General found that the SSA was vulnerable to potential error or fraud due to lack of segregation of duties within hospitals' birth registration units and found instances where multiple SSNs were issued to a child or where SSNs were issued to unnamed children (e.g., with name listed as "Baby" or "Infant").

The SSA Inspector General recommended that the SSA perform periodic independent reconciliations of registered births with statistics obtained from the hospitals' labor and delivery units and periodically verify the legitimacy of a sample of birth records obtained from hospitals. The SSA Inspector General also recommended enhancement of routines to prevent assignment of multiple SSNs, additional training for SSA personnel, and continued monitoring and improvement of the timeliness of Bureau of Vital Statistics submissions.

Effective Date:

The Commissioner would be required to report to Congress on the extent to which such improvements have been made no later than one year after enactment.

The Commissioner would be required to report the results of the study to the House Committee on Ways and Means and the Senate Committee on Finance no later than 18 months after enactment.

Sec. 203. Study relating to use of photographic identification in connection with applications for benefits, Social Security account numbers, and Social Security cards.

Current Law:

Individuals must submit proof of age, U.S. citizenship or lawful alien status, and identity when applying for an SSN or Social Security benefits (additional evidence is required for benefit applications). Persons applying for a replacement SSN card must submit proof of identity and may be required to submit proof of age and U.S. citizenship or lawful alien status. An in-person interview is required for SSN applicants age 12 and older and may be required for other applicants.

Examples of documents that may be submitted as proof of identity include a driver's license, marriage or divorce record, life insurance policy or passport. Photo identification is preferred but not required.

Explanation of Provision:

The bill would require the Commissioner to undertake a study to determine the best method by which to (a) require and obtain photo identification of persons applying for Social Security benefits, an SSN, or a replacement SSN card, and (b) provide reasonable exceptions to this requirement to promote efficient and effective administration of the Social Security program.

In addition, the study would be required to include an evaluation of the costs and benefits of photo identification, including the degree to which the security and integrity of the Social Security program would be enhanced.

Reason for Change:

The SSA has conducted pilot projects in which the agency requested photographic identification from individuals filing for Social Security or SSI benefits based on a disability or blindness. The purpose was to gather information on the use of photographic identification to address the issue of complicit impersonation in the disability claims process. However, SSN issuance and other benefit applications are also vulnerable to fraud, and requiring photographic identification in these circumstances should be studied as well.

Effective Date:

The Commissioner would be required to report the results of the study to the House Committee on Ways and Means and the Senate Committee on Finance no later than 18 months after enactment.

Sec. 204. Restrictions on issuance of multiple replacement Social Security cards.

Current Law:

Federal regulations specify that, in the case of a lost or damaged Social Security card, a duplicate card bearing the same name and number may be issued. In the case of a name change, a corrected card bearing the same number and new name may be issued. SSA policy allows individuals to obtain up to 52 replacement cards per year, with no lifetime limit.

Explanation of Provision:

The bill would require the Commissioner to restrict issuance of replacement SSN cards issued to any individual to 3 per year and 10 for life, except in cases where the Commissioner determines there is minimal opportunity for fraud.

Reason for Change:

Of the nearly 18 million SSN cards issued in fiscal year 2003, more than 12 million (69 percent) were replacement cards. In testimony before the Committee on Ways and Means, Subcommittee on Social Security, the GAO stated that the SSA's policy for replacing Social Security cards increases the potential for misuse of SSNs, and recommended limiting replacement SSN card issuance. The ability to obtain numerous replacement SSN cards increases the vulnerability that requestors may obtain SSNs for a wide range of illicit uses, including selling them to non-citizens to enable them to work or to individuals seeking to hide their identity.

The SSA Inspector General also stated that the SSA is at risk from individuals who misuse replacement SSN cards. In a 2001 audit, the SSA Inspector General found irregularities among a sample of individuals issued 3-6 replacement cards within a year, which indicated the individuals obtained replacement cards for suspect reasons. These irregularities included SSN holders who had earnings higher than would be expected given the individual's age, number of employers, and type of employment; an improbable number of replacement cards issued based on the individual's age; wages reported under the individual's SSN but not the individual's name as stated on the card issued; and individuals with earnings who were also drawing disability benefits. The SSA Inspector General recommended restricting issuance of replacement SSN cards to an individual to 3 per year and 10 over an individual's lifetime.

Effective Date:

The Commissioner would be required to issue regulations no later than one year after enactment.

Sec. 205. Study relating to modification of the Social Security account numbering system to show work authorization status.

Current Law:

SSN cards issued to persons other than U.S. citizens or persons lawfully admitted to the U.S. with permanent work authorization from the Department of Homeland

Security (DHS) (which subsumed the former Immigration and Naturalization Service [INS]) are annotated to indicate the individual's work authorization status, as follows:

> (1) SSN cards issued to persons lawfully admitted to the U.S. on a temporary basis with DHS work authorization are inscribed "VALID FOR WORK ONLY WITH INS AUTHORIZATION."
>
> (2) SSN cards issued to persons lawfully admitted to the U.S. without DHS work authorization are inscribed "NOT VALID FOR EMPLOYMENT." Such persons may be assigned an SSN only for valid non-work purposes, such as when Federal statute or regulation requires an SSN to receive Federally-funded benefits, or when a State or local law requires an SSN to receive general public assistance benefits.

While SSN cards (and SSA records) are annotated to indicate an individual's work authorization status at the time a number is assigned in cases described above, the current Social Security numbering system does not reflect an individual's work authorization status.

Explanation of Provision:

The bill would require the Commissioner, in consultation with the Secretary of Homeland Security, to undertake a study to determine the best method by which to modify SSNs assigned to persons who (1) are not United States citizens, (2) have not been admitted for permanent residence, and (3) are not legally authorized to work in the United States or are authorized to work in the United States with restriction, to indicate the individual's work authorization status.

Reason for Change:

Employers are required to solicit a worker's SSN in order to report their wages and pay Social Security taxes. A worker may also submit the SSN card as part of the proof required by the Department of Homeland Security (Form I-9) that an individual is authorized to work in the United States.

However, employers are not required to see the SSN card, nor are they required to verify a verbally-provided SSN with the SSA or confirm work authorization by contacting the Department of Homeland Security. Since SSNs may be issued for non-work purposes in limited situations, or based on temporary work authorization, modifying the SSN itself to indicate whether or not it was issued based on permanent authorization to work could potentially help employers determine whether an individual is truly authorized to work in the United States without placing additional documentation burdens on them.

Effective Date:

The Commissioner would be required to report the results of the study to the Committee on Ways and Means and the Committee on Finance no later than one year after enactment.

TITLE III--ENFORCEMENT

Sec. 301. New criminal penalties for misuse of Social Security account numbers.

Current Law:

Section 208 of the Social Security Act provides criminal penalties for fraudulently obtaining an SSN from the SSA or the misuse of an SSN. In such cases, Section 208 specifies that persons shall be guilty of a felony and upon conviction shall be fined under Title 18, United States Code (up to $250,000 for an individual and up to $500,000 for an organization) and/or imprisoned for up to five years.

In addition, depending upon the facts, certain sections under Title 18 of the United States Code are applicable to the misuse of SSNs, including 18 U.S.C § 1028(a)(7), the "Identity Theft and Assumption Deterrence Act of 1998" (P.L. 105-318), which prohibits the knowing transfer or use of another person's SSN without lawful authority. The "Internet False Identification Prevention Act of 2000" (P.L. 106-578) closed some loopholes in the "Identity Theft and Assumption Deterrence Act of 1998" by prohibiting the transfer of a false identification document by electronic means, including on a template or computer file or disc and repealed provisions of the Federal criminal code prohibiting the mailing of private identification documents without a disclaimer noting that such documents are not government produced.

The "Identity Theft Penalty Enhancement Act" (P.L. 108-275) establishes penalties for aggravated identity theft. The law prescribes sentences, to be imposed in addition to the punishments provided for the related felonies, of: (1) Two years' imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations; and (2) five years' imprisonment for knowingly taking such action with respect to a means of identification or a false identification document during and in relation to specified felony violations pertaining to terrorist acts. The law also prohibits a court from: (1) Placing any person convicted of such a violation on probation; (2) reducing any sentence for the related felony to take into account the sentence imposed for such a violation; or (3) providing for concurrent terms of imprisonment for a violation of the Act and a violation under any other Act.

Also, the new law expands the previous identify theft prohibition to: (1) Cover possession of a means of identification of another with intent to commit specified unlawful activity; (2) increase penalties for violations; and (3) include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism.

Lastly, P.L. 108-275 law modifies provisions regarding embezzlement and theft of public money, property, or records to provide for combining amounts from all the counts for which the defendant is convicted in a single case for purposes of determining which penalties apply.

Explanation of Provision:

The bill would expand the types of SSN misuse to which criminal penalties apply. Specifically, the bill would provide criminal penalties for persons who: (1) disclose, sell or transfer their own SSN with intent to deceive; (2) offer, for a fee, to improperly acquire or help improperly acquire an additional SSN for an individual; (3) violate the prohibition on display of SSNs on employee identification cards or tags created under Section 105 of this bill; (4) violate the prohibitions the bill would establish under Sections 101, 103, 104, 105, 106, or 107 of this bill (with respect to officers or employees of any Federal, State or local agency); or (5) violate Sections 101, 103, or 107 of this bill (with respect to bankruptcy trustees). (Note: the penalties for violations of Section 108 are included in Section 108 of the bill.)

Reason for Change:

Identity theft often begins with the misuse of an SSN. While advances have been made to prosecute those individuals who assist another person to improperly acquire an additional SSN or a number that purports to be an SSN, the SSA Inspector General and the Department of Justice have continued to encounter some problems, for example in prosecuting individuals who operate over the Internet or at a flea market. It is appropriate to close loopholes to prevent individuals assisting another person to improperly acquire an additional SSN or a number that purports to be an SSN. In addition, it is appropriate to establish penalties for those who violate the prohibitions on sale, purchase and display to the general public established under this bill.

In addition, the SSA Inspector General has investigated individuals who have sold or transferred their own SSN to a third person with intent to deceive and has encountered problems in the prosecution. While such an individual may potentially be prosecuted under the criminal statutes involving conspiracy or aiding and abetting, because of the gravity of SSN misuse, it is appropriate to address this problem head on and provide criminal penalties when an individual sells or transfers their SSN with intent to deceive.

Effective Date:

The criminal penalty would apply to violations that occur after enactment, except for violations under Title I of this bill. In such cases, the criminal penalty would apply to violations that occur on or after the applicable effective date.

Sec. 302. Extension of civil monetary penalty authority.

Current Law:

Section 1129 of the Social Security Act (42 U.S.C. § 408) authorizes the Commissioner to impose civil monetary penalties and assessments on any person who makes a false statement or representation of a material fact, or omits a material fact while providing a statement, for use in determining eligibility for Social Security or SSI benefits or benefit amount. The Commissioner may impose a civil monetary penalty of up to $5,000 for each violation, and an assessment of up to twice the amount of benefits or payments paid as a result of such violation.

Currently, an individual who improperly obtains an SSN from SSA or misuses another person's SSN is not subject to civil monetary penalties and assessments under Section 1129, except in cases of SSN misuse related to the receipt of Social Security or SSI benefits.

Explanation of Provision:

The bill would expand the types of activities to which civil monetary penalties and assessments apply. Specifically, it would authorize the Commissioner to impose (in addition to any other penalties that may apply) civil monetary penalties and assessments on persons who: (1) Use an SSN obtained through false information; (2) falsely represent an SSN to be their own; (3) alter an SSN card; (4) buy or sell an SSN card; (5) counterfeit an SSN card; (6) disclose, use or compel the disclosure of the SSN of any person in violation of any Federal law; (7) provide false information to obtain an SSN; (8) offer to acquire, for a fee, an additional SSN for an individual; (9) disclose, sell or transfer a person's own SSN with intent to deceive; (10) violate Sections 101, 103, 104, 105, 106, or 107 of this bill (with respect to officers or employees of a Federal, State or local agency); (11) violate Sections 101, 103, or 107 of this bill (with respect to bankruptcy trustees); (12) violate Section 108 of this bill; or (13) violate Section 303 of this bill (with respect to SSA employees).

Reason for Change:

SSN misuse, not related to the determination of eligibility for, or the amount of, Social Security or SSI benefits, can also result in considerable costs for the government,

the private sector, and individuals who are victims of fraud. In many cases, the costs of SSN misuse extend beyond monetary losses.

The SSN is a valuable commodity today for criminals. As the Subcommittee has heard in testimony, the use of the SSN has grown so that it is interwoven into many aspects of every day life. It has become the *de facto* national identifier, used as a "breeder document" to obtain a driver's license or a credit card, open a bank account or secure a loan.

Because of the prevalence of the use of the SSN in society and the gravity of SSN misuse, it is appropriate to provide for civil monetary penalties and assessments for violations of the law relating to SSN misuse in general.

Effective Date:

The civil monetary penalties would apply to violations that occur after enactment, except with respect to violations of prohibitions created under this bill. In such cases, the civil monetary penalties would apply to violations that occur on or after the applicable effective date.

Sec. 303. Criminal penalties for employees of the Social Security Administration who knowingly and fraudulently issue Social Security cards or Social Security account numbers.

Current Law:

SSA employees who fraudulently sell SSNs to third parties may be tried under a number of criminal statutes, including but not limited to 18 U.S.C. § 371 (conspiracy) and 18 U.S.C. § 641 (theft of government property).

Explanation of Provision:

The bill would provide for mandatory minimum criminal penalties for SSA employees (including contract workers, State Disability Determination Service workers and volunteers in an SSA facility) who knowingly and fraudulently sell or transfer SSNs or Social Security cards, with the penalty based on the *number* of SSNs or Social Security cards fraudulently issued, as follows: 1) 1 to 50 SSNs or cards: 1-5 years imprisonment; 2) 51 to 100 SSNs or cards: 5-10 years imprisonment; or 3) 101 or more SSNs or cards: 10-20 years imprisonment.

In addition, the bill would apply the same penalties to an SSA employee who attempts or conspires to commit a violation of this section.

Reason for Change:

Crimes of fraud against the integrity of the SSN are of great concern because of the far reaching implication such crimes have upon the integrity of the SSA, the potential impact on innocent individuals due to identity theft, and possible misuse of SSNs in terrorist activities. This is especially true when the crime is perpetrated, at least in part, by a SSA employee. SSA employees issuing SSNs are in a position of trust. When this trust is violated, the effect on the SSA's programs and operations and on the public in general can be devastating. Fortunately, the number of SSA employees taking part in these crimes is small, but participation in such crimes by any SSA employee to any extent cannot be tolerated.

The SSA and the SSA Inspector General are concerned that current laws do not provide an adequate deterrent to SSA employees tempted to facilitate these crimes. In several recent investigations involving SSA employees, the employee when caught, has received little, if any, prison time though the employee may have fraudulently issued hundreds of SSNs. The Committee is concerned because the SSNs issued have usually not previously been issued to anyone else. Even a thorough credit check would not show this SSN to be fraudulent. This could allow a criminal to more easily assimilate into our society. Therefore, it is appropriate to provide for enhanced criminal penalties for SSA employees who assist in the fraudulent issuance of SSNs.

Effective Date:

The penalties would apply to violations that occur on or after enactment.

Sec. 304. Enhanced penalties in cases of terrorism, drug trafficking, crimes of violence, or prior offenses.

Current Law:

Sections 208, 811 and 1632 of the Social Security Act (regarding Social Security benefits, Special Benefits for Certain WWII Veterans and SSI benefits, respectively) provide that persons who willingly and knowingly commit fraud shall be guilty of a felony and upon conviction shall be fined under Title 18, United States Code, and/or imprisoned for up to five years.

Examples of violations to which penalties apply include making false statements or representations of fact to obtain benefits or increase benefit payments; failing to disclose an event that affects an individual's initial or continued right to receive benefits; and engaging in various types of SSN misuse or fraud (such as using an SSN obtained on the basis of false information; falsely representing an SSN to be one's own with intent to

deceive; buying or selling an SSN card; counterfeiting an SSN card; or disclosing, using or compelling the disclosure of the SSN of any person in violation of any Federal law).

Penalties apply to violations committed by individuals (or organizations) acting in the capacity of a representative payee (or prospective representative payee) for a beneficiary other than the individual's spouse. If the court determines that the violation also includes willful misuse of funds, the court may require full or partial restitution of funds to the beneficiary.

Explanation of Provision:

The bill would enhance criminal penalties under Sections 208, 811 and 1632 of the Social Security Act with respect to (a) repeat offenders and (b) violations committed to facilitate a drug trafficking crime, a crime of violence, or an act of international or domestic terrorism.

Specifically, the bill would provide for (1) fines and/or imprisonment for up to five years for first offenders; (2) fines and/or imprisonment for up to 10 years for repeat offenders; (3) fines or imprisonment for up to 20 years for persons convicted of violations for the purpose of facilitating a drug trafficking crime or a crime of violence; and (4) fines or imprisonment for up to 25 years for persons convicted of violations for the purpose of facilitating an act of international or domestic terrorism.

Reason for Change:

The expanded use of the SSN in today's society has made it a very valuable commodity for criminals. As the Subcommittee has heard in several hearings, the SSN is considered a prime "breeder document", a valuable commodity used to obtain a driver's license or credit cards, as well as open a bank account or obtain a loan. But in addition to being a lynchpin for identity theft crimes, it also assists terrorists in assimilating into our society and avoiding detection.

The integrity of the SSN is vital. Its importance in both identity theft and homeland security is universally recognized. Providing new, enhanced, structured penalties appropriately reflects the vital importance of the SSN and the commitment of the Congress, the SSA and the SSA Inspector General to its protection.

Effective Date:

Would apply to violations that occur after enactment.

III. VOTE OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the following statements are made concerning the vote of the Committee on Ways and Means in its consideration of the bill, H.R. 2971.

MOTION TO REPORT THE BILL

The bill, H.R. 2791, as amended, was ordered favorably reported by a roll call vote of 33 yeas to 0 nays (with a quorum being present). The vote was as follows:

Representatives	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Thomas.....	√			Mr. Rangel.....	√		
Mr. Crane.....	√			Mr. Stark.....			
Mr. Shaw.....	√			Mr. Matsui.....			
Mrs. Johnson.....	√			Mr. Levin.....	√		
Mr. Houghton.....	√			Mr. Cardin.....	√		
Mr. Herger.....	√			Mr. McDermott.....	√		
Mr. McCrery.....	√			Mr. Kleczka.....	√		
Mr. Camp.....	√			Mr. Lewis (GA).....			
Mr. Ramstad.....	√			Mr. Neal.....	√		
Mr. Nussle.....				Mr. McNulty.....			
Mr. Johnson.....	√			Mr. Jefferson.....	√		
Ms. Dunn.....	√			Mr. Tanner.....	√		
Mr. Collins.....				Mr. Becerra.....	√		
Mr. Portman.....	√			Mr. Doggett.....	√		
Mr. English.....	√			Mr. Pomeroy.....	√		
Mr. Hayworth.....				Mr. Sandlin……..			
Mr. Weller.....	√			Ms. Tubbs Jones….	√		
Mr. Hulshof.....	√						
Mr. McInnis.....	√						
Mr. Lewis (KY).....	√						
Mr. Foley.....	√						
Mr. Brady.....	√						
Mr. Ryan.....	√						
Mr. Cantor……..	√						

IV. BUDGET EFFECTS OF THE BILL

A. COMMITTEE ESTIMATE OF BUDGETARY EFFECTS

In compliance with clause 3(d)(2) of rule XIII of the Rules of the House of Representatives, the following statement is made concerning the effects on the budget of this bill, H.R. 2971 as amended and reported: The Committee agrees with the estimate prepared by the Congressional Budget Office (CBO), which is included below.

B. STATEMENT REGARDING NEW BUDGET AUTHORITY AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee states that H.R. 2971 does not include any new budget authority or tax expenditures.

C. COST ESTIMATE PREPARED BY THE CONGRESSIONAL BUDGET OFFICE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, requiring a cost estimate prepared by the Congressional Budget Office, the following report by CBO is provided.

[to be provided by CBO]

V. OTHER MATTERS TO BE DISCUSSED UNDER THE RULES OF THE HOUSE

A. COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives (relating to oversight findings), the Committee, based on public hearing testimony, conclude that it is appropriate and timely to consider the bill as reported.

B. STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

With respect to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee advises that the Administration has in place program goals and objectives, which have been reviewed by the Committee. H.R. 2971 includes provisions to assist the Administration in achieving its goals to prevent SSN misuse and strengthen the integrity of SSNs.

CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

August 18, 2004

H.R. 2971
Social Security Privacy and Identity Theft Prevention Act of 2004

As ordered reported by the House Committee on Ways and Means on July 21, 2004

SUMMARY

H.R. 2971 would provide new safeguards for the use of Social Security numbers (SSNs) and penalties for SSN misuse. The bill would:

- Bar the sale, purchase, or display of the SSN in both the public and private sectors, with certain exceptions;
- Prohibit the display of SSNs (including magnetic strips or bar codes that contain them) on government checks, drivers' licenses, and motor vehicle registrations, employer-issued identification cards or tags, and cards used to gain access to employee benefits or services;
- Require government and private entities to limit access to SSNs and assure that they have safeguards to prevent breaches of confidentiality;
- Tighten some procedures that the Social Security Administration (SSA) follows when issuing new or replacement SSNs, and require SSA to study further improvements; and
- Create or expand civil and criminal penalties for SSN misuse.

Implementing H.R. 2971 could affect direct spending and revenues, but CBO estimates that any such effects would not be significant. Complying with the bill's standards would also cause federal agencies to incur additional administrative expenses. Those costs—which CBO estimates at $3 million over the 2005-2009 period—would generally come from agencies' salary and expense budgets, which are subject to annual appropriation.

H.R. 2971 contains a number of intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), including limitations on the sale, display, and use of SSNs by state, local, and tribal governments. While there is some uncertainty about the aggregate

costs of complying with those mandates on those governments, CBO estimates that they likely would exceed the intergovernmental threshold established in UMRA ($60 million in 2004, adjusted annually for inflation) in at least one of the first five years following the date the mandates go into effect.

H.R. 2971 also would impose private-sector mandates, as defined in UMRA, on certain private entities and consumer reporting agencies. CBO cannot determine the total direct costs of complying with those mandates because the costs would depend on specific regulations that would be issued to implement the bill.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 2971 is shown in the following table. For this estimate, CBO assumes that the bill will be enacted in the fall of 2004. The costs of the legislation fall primarily in functions 650 (Social Security) and 750 (administration of justice) but—because all government agencies use the SSN—affect numerous other budget functions as well. As explained below, CBO cannot estimate some potential costs in cases where agencies do not yet know how they would implement certain provisions.

	By Fiscal Year, in Millions of Dollars				
	2005	2006	2007	2008	2009
CHANGES IN SPENDING SUBJECT TO APPROPRIATION [a]					
Estimated Authorization Level	1	1	*	*	*
Estimated Outlays	1	1	*	*	*

NOTE: * = Less than $500,000.

a. Enacting H.R. 2971 could also affect direct spending and revenues, but CBO estimates that any such effects would not be significant.

BASIS OF ESTIMATE

Federal agencies already comply, or are moving to comply, with most requirements of H.R. 2971. The budgetary effects thus stem from a few provisions that would change agencies' practices or assign new enforcement responsibilities.

Current law

Federal agencies are allowed—in fact, are usually required—to collect SSNs, but the Privacy Act bars the government from selling or renting SSNs or disclosing them (with certain exceptions) without the subjects' written consent. Agencies also must justify any matching agreements involving computerized records (for example, those that intercept tax refunds of people who have defaulted on government loans), must ensure computer security, and must post their privacy policies when conducting business electronically with the public.

H.R. 2971 would require agencies that accept SSNs electronically from the public to ensure that the number is encrypted or "otherwise appropriately secured from disclosure." SSA and the Internal Revenue Service—which process millions of reports that contain SSNs—now use encryption or are phasing out the few exceptions. No law now requires encryption, however, so some lower-volume users may use less-advanced technology.

The Treasury Department's Financial Management Service no longer shows SSNs on checks, except in a few cases dictated by states' needs. Identification tags issued to federal civilian employees generally do not show or contain the SSN.

Spending Subject to Appropriation

Social Security Administration and Department of Justice. H.R. 2971 would give specific new responsibilities to SSA and the Department of Justice. It would direct SSA to independently verify birth records for SSN applicants, except for babies who get SSNs through the Enumeration at Birth program. SSA already does so for applicants more than 1 year old, so extra costs would be insignificant. H.R. 2971 also would require SSA to prepare several studies and reports, notably on a possible requirement for photo identification when people apply for benefits or replacement SSN cards and on revising the account numbering system to reflect the work authorization of immigrants. The Department of Justice would take the lead in drafting regulations to govern compliance with the new law in both the public and private sectors and would prosecute violations. Based on the scope of the agencies' new tasks, CBO estimates costs of $2 million over the 2005-2009 period, assuming the availability of appropriated funds.

That estimate contains a major caveat, however. H.R. 2971 would require all federal agencies to demonstrate to SSA that they allow access only to employees who need SSNs to carry out their statutory responsibilities and have safeguards to prevent unauthorized access and breaches of confidentiality. The provision would apply to all SSNs in the agencies' possession, including paper records, not just to computerized systems. Its implications for contractors (who handle key responsibilities especially in the areas of

welfare and child support enforcement) are unclear. According to the General Accountability Office (GAO), every federal agency uses the SSN in some way. CBO cannot estimate the cost of this provision to SSA or to other agencies because it would depend on SSA's approach.

Department of Defense. The bill would ban the display of SSNs on employee identification cards. The Geneva Convention calls for military personnel to have a number displayed on their identification cards, and the Department of Defense has chosen to use the SSN. Under the bill, it would have to revamp its records and cards to use another unique identifier for its 2.7 million active-duty and reserve forces. Because DOD cannot determine at this time how it would implement the provision, CBO cannot estimate the cost, but it could be quite large.

Employee Benefits. H.R. 2971 would bar administrators of employee-benefit plans (such as health insurers) from displaying the SSN on identification or membership cards. Some plans that participate in the Federal Employees Health Benefits (FEHB) program show the SSN on membership cards. Although the ban would technically apply only to cards issued one year after issuance of regulations, or about 30 months after enactment, CBO assumes that the affected plans would issue replacement cards to current members as well. (Changes to plans' administrative costs would likely be recouped through higher premiums charged to FEHB enrollees.) Because the government subsidizes FEHB premiums, it would bear part of the cost; CBO estimates the extra cost to the federal government would be less than $500,000. (About half would come from agencies' salary and expense accounts on behalf of current employees, but the rest would be paid on behalf of annuitants and would constitute direct spending.) CBO expects that the provision would not apply to the government's Medicare program, which shows the SSN on the cards of its 42 million enrollees.

Direct Spending and Revenues

Civil and Criminal Penalties. Title III of H.R. 2971 would add or toughen civil and criminal penalties for SSN misuse. The Commissioner of Social Security (with permission from the Attorney General) could impose civil penalties of as much as $5,000 per offense; criminal penalties require a court conviction and may be as high as $250,000. Criminal fines are deposited in the Crime Victims Fund and later spent; consequently, over time, they have little net effect on the budget. Collections of civil fines are recorded as revenues and deposited in the Treasury. The penalties would apply to offenses committed after enactment, and CBO judges that they would not be significant over the 2005-2009 period.

Regulatory Agencies. Title I would direct the Commissioner of SSA and the Attorney General to consult with—among others—various banking and regulatory agencies when crafting regulations to end the sale or display of SSNs in the public and private sectors. The

Federal Reserve earns interest on its holdings of government securities and subtracts its operating costs before remitting the rest to the Treasury as a revenue. Several other agencies—the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, and so forth—cover their costs through fees or assessments. CBO expects that those agencies would not incur significant costs as a result of H.R. 2971, so that any effect on direct spending or revenues would be negligible.

Child Support Enforcement. Requiring government agencies to remove SSNs from checks could raise administrative costs to the child support enforcement (CSE) program or delay distribution of collections. Many states currently use SSNs as their primary identifier when distributing child support, and the federal government covers the bulk of states' costs for administering CSE. However, CBO judges that the requirement would only have a small impact on the federal budget.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 2971 contains a number of intergovernmental mandates as defined in UMRA. Specifically, the bill would restrict or prohibit governmental agencies from:

- Selling or displaying Social Security numbers that have been disclosed to the agency because of a mandatory requirement (applicable only to documents issued after the requirements become effective);

- Displaying SSNs on checks or check stubs;

- Placing SSNs on drivers licenses, identification cards, vehicle registrations, or employee identification cards, or coding them into magnetic strips or bar codes on those documents; and,

- Allowing prisoners access to SSNs of other individuals.

The bill also would require state and local governments to restrict access to SSNs and their derivatives to employees whose access is essential to effective administration of programs. In addition, the governments must implement safeguards to preclude unauthorized access to SSNs and their derivatives and to protect individual confidentiality.

While state and local governments have, in recent years, taken steps to reduce the use of SSNs, many continue to use them for a variety of purposes. Based on information from the GAO and discussions with state and local officials, CBO estimates that the costs of complying with the mandates in the bill likely would exceed the intergovernmental threshold

established in UMRA ($60 million in 2004, adjusted annually for inflation) in at least one of the first five years following the date the mandates go into effect.

Exceptions and Requirements

The bill would allow exceptions for the display or sale of SSNs when such use or display is authorized by the Social Security Act; necessary for law enforcement, national security, or tax law purposes; done in compliance with certain motor vehicle laws or consumer reporting practices; or for non-market research for advancing the public good. The bill's restrictions on the sale or display (which includes Internet transmissions that are not encrypted or otherwise secured) of SSNs would be prospective, and would not require state and local governments to redact SSNs from existing publicly available documents.

However, if state and local governments do not currently have a system in place to safeguard SSNs, they would have to implement a new system for any documents issued when the regulations become effective (up to two and a half years following enactment). If state or local governments use SSNs on checks and check-stubs as part of their recordkeeping and tracking procedures, they would have to alter those systems and remove the SSNs. They also would have to implement systems for removing SSNs from many documents that include SSNs and that are available to the public. Likewise, some states may have to alter their document systems for driver licenses and vehicle registrations to remove SSNs that are coded electronically onto a magnetic strip or digitized as part of a bar code. Finally, any government agency that uses SSNs would have to implement safeguards to preclude unauthorized access to SSNs and their derivatives and to protect confidentiality.

Potential Costs to State, County, and Municipal Governments

Because of the large number of governments affected by these provisions (particularly municipal governments), even small changes to existing systems would result in costs that exceed the threshold established in UMRA. There are over 75,000 municipal governments, so even small one-time costs—for example, as little as $5,000—would add up to costs over $60 million in a given year. Counties and states, on the other hand, while fewer in number (there are about 3,600 counties in the United States) are more dependent on SSNs for various recordkeeping and identification purposes and are thus likely to face significantly higher costs because of the complexity and scope of their recordkeeping systems. (Some counties

estimate that altering their systems to use identifiers other than SSNs or to eliminate display of SSNs would result in one-time costs ranging from $40,000 to over $1 million, depending on the scope of the changes that would need to be made).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 2971 would impose private-sector mandates, as defined in UMRA, on certain private entities and consumer reporting agencies. CBO cannot determine the total direct costs of complying with those mandates because such costs would depend on the specific regulations that would be issued under the bill.

Prohibition of the Sale, Purchase, and Disclosure of Social Security Numbers

The bill would impose a private-sector mandate on certain private entities by generally prohibiting the purchase, sale, or display of a Social Security number to the general public, including the display of an SSN on any card or tag issued to another person to provide access to any goods, services, or benefits. Private entities also would be prohibited from displaying SSNs on employee identification cards or tags (including on magnetic strips and bar codes.) In addition, private entities that maintain SSNs in their records for the conduct of their business would be required to limit access to those records and institute safeguards to protect the confidentiality of those records. The Commissioner of Social Security would issue regulations specifying the safeguards that would be required. CBO cannot estimate the direct cost to private entities of complying with those mandates.

Refusal To Do Business Without Receipt of Social Security Numbers

The bill would impose a new private-sector mandate by prohibiting certain private entities from refusing to do business with an individual because the individual will not provide his or her SSN. Such private entities that refuse to do business would be considered to have committed an unfair or deceptive act or practice in violation of federal trade law and would be subject to penalties. The cost of the mandate would be the incremental amount required to complete a business transaction without using a Social Security number for identification or credit verification. For example, a business may incur additional costs in verifying the credit worthiness of a person without an SSN for identification. According to the Federal Trade Commission and industry sources, few private entities currently refuse to do business if an individual does not provide his or her Social Security number. Therefore, CBO estimates that the direct cost to comply with the mandate would be small.

Prohibition of Social Security Numbers in Credit Header Information

The bill also would impose a private-sector mandate on consumer reporting agencies by prohibiting such agencies from providing Social Security numbers, or any derivative of such

numbers, except in a full consumer report furnished in accordance with the Fair Credit Reporting Act. The direct cost of the mandate would be the net income lost to consumer reporting agencies from not furnishing a consumer's Social Security number in the credit header information they sell to customers. According to industry sources, such agencies expect only a slight decrease in the sales of credit header information. Therefore, CBO estimates that the direct cost to comply with the mandate would be small.

ESTIMATE PREPARED BY:

Federal Costs: Kathy Ruffing (SSA)
Julia Christensen (FEHB)
Sheila Dacey (Child Support Enforcement)
Kathleen Gramp (Banking Agencies)
Mark Grabowicz (Justice)
Matthew Pickford (Treasury)
Michelle Patterson (Defense)

Impact on State, Local, and Tribal Governments: Leo Lex

Impact on the Private Sector: Paige Piper-Bac and Ralph Smith

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis

C. CONSTITUTIONAL AUTHORITY STATEMENT

With respect to clause (3)(d)(1) of rule XIII of the Rules of the House of Representatives, relating to Constitutional Authority, the Committee states that the Committee's action in reporting the bill is derived from Article I of the Constitution, Section 8 (`The Congress shall have power to lay and collect taxes, duties, imposts, and excises, to pay the debts and to provide for * * * the general Welfare of the United States.')

D. INFORMATION RELATING TO UNFUNDED MANDATES

This information is provided in accordance with Section 423 of the Unfunded Mandates Reform Act of 1995 (P.L. 104-4).

The Committee has determined that the bill does impose a Federal intergovernmental mandate on State, local, or tribal governments. The Committee has determined that the bill does contain Federal mandates on the private sector.

VI. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

[to be provided by the Office of Legislative Counsel]